

(19) World Intellectual Property Organization  
International Bureau(43) International Publication Date  
21 March 2002 (21.03.2002)

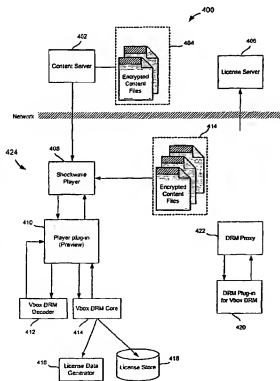
PCT

(10) International Publication Number  
WO 02/023315 A3

- (51) International Patent Classification<sup>7</sup>: G06F 1/00
- (21) International Application Number: PCT/US01/26495
- (22) International Filing Date: 24 August 2001 (24.08.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
09/659,902 12 September 2000 (12.09.2000) US
- (71) Applicant: ALADDIN KNOWLEDGE SYSTEMS, LTD. (IL/IL); 15, Beit Oved Street, Tel Aviv 61110 (IL).
- (72) Inventors: XU, Bin; 955 La Mesa Terrace, Unit-I, Sunnyvale, CA 94086 (US). LI, Weijun; 687 Ontario Court, # 8, Sunnyvale, CA 94087 (US). SMITH, Kyle; 394 Vale Drive, San Jose, CA 95123 (US). BAO, Dalun; 200 E. Dana St. D85, Mountain View, CA 94041 (US).
- (74) Agents: NWAMU, Fidel, D. et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, Eighth Floor, San Francisco, CA 94111 (US).
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEM FOR MANAGING RIGHTS AND PERMITTING ON-LINE PLAYBACK OF DIGITAL CONTENT



(57) Abstract: A system for managing the rights to one or more digital content files within a computer network, and for permitting the on-line playback of such content files by an authorized user. In order to manage these rights, the system encrypts the content files to prevent unauthorized access to the files. Encryption is accomplished by using one or more keys which are associated with one or more segments of the content file. These keys enable an authorized user to decrypt and playback the content files at a subsequent time. Upon receiving the keys, an end user's system retrieves a license from a license server which specifies the rights of the user as it relates to the content files.

WO 02/023315 A3

**Published:**

— with international search report

**Previous Correction:**

see PCT Gazette No. 51/2002 of 19 December 2002, Section II

(88) Date of publication of the international search report:

7 August 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(15) Information about Correction:

## INTERNATIONAL SEARCH REPORT

International Publication No.  
PCT/US 01/26495A. CLASSIFICATION OF SUBJECT MATTER  
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EP0-Internal, WPI Data, PAJ

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 42098 A (CRYPTOWORKS INC) 24 September 1998 (1998-09-24) figure 1 abstract page 1, line 5 - line 6 page 1, line 11 - line 13 page 5, line 16 - line 18 page 5, line 20 - line 24 page 5, line 33 - page 6, line 2 page 6, line 6 - line 20 page 9, line 29 - line 30 page 10, line 11 - line 17 page 10, line 25 - line 32 page 11, line 3 - line 5 page 11, line 8 - line 15 page 14, line 22 - line 23 page 15, line 3 - line 4 page 15, line 7 - line 9 page 16, line 13 - line 15 -/--	1-15

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

## \* Special categories of cited documents:

\*A\* document defining the general state of the art which is not considered to be of particular relevance

\*E\* earlier document but published on or after the international filing date

\*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

\*O\* document referring to an oral disclosure, use, exhibition or other means

\*\*P\* document published prior to the international filing date but later than the priority date claimed

\*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

\*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

\*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

\*&amp;\* document member of the same patent family

Date of the actual completion of the international search

31 January 2003

Date of mailing of the international search report

10/02/2003

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentstra 2  
NL - 2280 HV Rijswijk  
Tel (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+31-70) 340-3016

Authorized officer

Chabot, P

## INTERNATIONAL SEARCH REPORT

International Application No.

PCT/US 01/26495

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	<p>page 16, line 18 - line 28  page 16, line 31 -page 17, line 2  page 17, line 6 - line 9  page 17, line 13 - line 20  page 17, line 26 - line 27  page 18, line 19 - line 34  page 19, line 12 - line 14  page 19, line 19 - line 21  page 20, line 14 - line 20  page 21, line 3 - line 12  page 21, line 20 - line 23  page 25, line 16 - line 21  page 26, line 13 - line 15  page 26, line 32 -page 27, line 2  page 28, line 4 - line 7  page 28, line 9 - line 23</p>	
A	<p>US 5 754 646 A (WILLIAMS THOMAS H ET AL)  19 May 1998 (1998-05-19)  column 2, line 51 -column 3, line 25  column 3, line 56 -column 4, line 29</p>	1-8
A	<p>US 5 222 134 A (WAITE DAVID P ET AL)  22 June 1993 (1993-06-22)  column 2, line 54 - line 68  column 3, line 57 - line 62  column 4, line 58 - line 63  column 4, line 66 - line 68</p>	1-8
A	<p>NOGHANI B S ET AL: "REDUCING LATENCY ON  THE INTERNET USING COMPONENT-BASED  DOWNLOAD AND FILE-SEGMENT TRANSFER  PROTOCOL: EXPERIMENTAL RESULTS"  PROCEEDINGS OF THE SYMPOSIUM OF  PERFORMANCE EVALUATION OF COMPUTER AND  TELECOMMUNICATION SYSTEMS, XX, XX,  16 July 2000 (2000-07-16), pages 324-331,  XP001012275  abstract</p>	1-16
A	<p>US 5 999 622 A (KUROSAWA TAKASHI ET AL)  7 December 1999 (1999-12-07)  abstract</p>	1-16

## INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No.

PCT/US 01/26495

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9842098	A	24-09-1998	AU 6759198 A EP 0968585 A1 WO 9842098 A1	12-10-1998 05-01-2000 24-09-1998
US 5754646	A	19-05-1998	CA 2227060 A1 GB 2317476 A ,B WO 9704412 A2	06-02-1997 25-03-1998 06-02-1997
US 5222134	A	22-06-1993	US 5103476 A AT 171024 T CA 2095723 A1 DE 69130175 D1 DE 69130175 T2 EP 0556305 A1 JP 7089345 B JP 6501120 T WO 9209160 A1	07-04-1992 15-09-1998 08-05-1992 15-10-1998 10-02-2000 25-08-1993 27-09-1995 27-01-1994 29-05-1992
US 5999622	A	07-12-1999	NONE	

## CORRECTED VERSION

(19) World Intellectual Property Organization  
International Bureau(43) International Publication Date  
21 March 2002 (21.03.2002)

PCT

(10) International Publication Number  
WO 02/023315 A2(51) International Patent Classification<sup>1</sup>: G06F 1/00

(21) International Application Number: PCT/US01/26495

(22) International Filing Date: 24 August 2001 (24.08.2001)

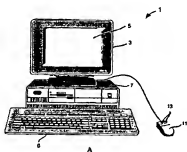
(25) Filing Language: English

(26) Publication Language: English

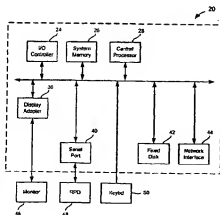
(30) Priority Date:  
09/659,902 12 September 2000 (12.09.2000) US(71) Applicant: ALADDIN KNOWLEDGE SYSTEMS,  
LTD. [IL/IL]; 15, Beit Oved Street, Tel Aviv 61110 (IL).(72) Inventors: XU, Bin; 955 La Mesa Terrace, Unit 1, Sunny-  
vale, CA 94086 (US); LI, Weijun; 687 Ontario Court, #8, Sunnyvale, CA 94087 (US); SMITH, Kyle; 394 Vale  
Drive, San Jose, CA 95123 (US); BAO, Dalan; 200 E.  
Dana St. D85, Mountain View, CA 94041 (US).(74) Agents: NWAMU, Fidel, D. et al.; Townsend and  
Townsend and Crew LLP, Two Embarcadero Center,  
Eighth Floor, San Francisco, CA 94111 (US).(81) Designated States (national): AE, AG, AL, AM, AT, AU,  
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,  
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,  
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,  
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,  
MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI,  
SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA,  
ZW.(84) Designated States (regional): ARIPO patent (GH, GM,  
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian

[Continued on next page]

(54) Title: SYSTEM FOR MANAGING RIGHTS AND PERMITTING ON-LINE PLAYBACK OF DIGITAL CONTENT



(57) Abstract: A system for managing the rights to one or more digital content files within a computer network, and for permitting the on-line playback of such content files by an authorized user. In order to manage these rights, the system encrypts the content files to prevent unauthorized access to the files. Encryption is accomplished by using one or more keys which are associated with one or more segments of the content file. These keys enable an authorized user to decrypt and playback the content files at a subsequent time. Upon receiving the keys, an end user's system retrieves a license from a license server which specifies the rights of the user as it relates to the content files.



WO 02/023315 A2



patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**(48) Date of publication of this corrected version:**

19 December 2002

**(15) Information about Correction:**

see PCT Gazette No. 51/2002 of 19 December 2002, Section II

**Published:**

— *without international search report and to be republished upon receipt of that report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

## SYSTEM FOR MANAGING RIGHTS AND PERMITTING ON-LINE PLAYBACK OF DIGITAL CONTENT

### BACKGROUND OF THE INVENTION

5           This invention relates to the field of information processing and more particularly to systems for implementing digital management rights.

          Millions of users currently have access to more information than at any period in the history of society. Specifically, digital content such as interactive web content, musical recordings, medical and financial forms, automatic banking, facsimiles,  
10       and various other forms of audio and video content are widely accessible.

          Although attributable to a number of reasons, the widespread access to digital content has been a result of the development of electronic computer networks, and Internet in particular. Another reason relates to the increase in available bandwidth and the availability of compression technology for transferring large amounts of content. In  
15       addition, numerous sites and bulletin boards post content for distribution to users. Content providers such as publishers of books and magazines, information database providers, and producers of music, video games, and images are distributing content in digital form over the Internet. In fact, some providers of interactive web content and music provide interactive web players for playing back content. Examples of such  
20       interactive web players which are currently available on the market are Quicktime 4™ available from Apple Computer, Inc.®, RealPlayer™ available from RealNetworks, Inc.® and Shockwave 7™ available from MacroMedia, Inc.®

          While access to digital content has been widely beneficial, a fundamental problem facing content providers is how to prevent the unauthorized use and distribution  
25       of digital content. Content providers are concerned with getting compensated for their work. Unauthorized copying and use of content providers works deprives rightful owners of billions of dollars according to a well-known source. Unauthorized copying is exacerbated because consumers can easily retrieve content, and technology is available for perfectly reproducing content.

30       A number of mechanisms have been developed to protect against unauthorized access and duplication and to provide digital rights management. One method is a digital rights management system that allows a set of rules to determine how the content is used. Another method (for software) for curbing unauthorized duplication



is the use of a scheme which provides software tryouts or demos that typically work and expire after a specific duration. Other methods use a copy protection scheme that limits the number of copies that a user can make, after which additional copying results in corrupt copies. Further, an alternate scheme requires the presence of a license on a client workstation for the software to operate.

Many of the aforementioned schemes are typically implemented using "encryption/decryption" of the digital content. Encryption is the conversion of data into an unintelligible form, e.g., ciphertext, that cannot be easily understood by unauthorized users. Decryption is the process of converting encrypted content back into its original form such that the it becomes intelligible. Simple ciphers include the rotation of letters in the alphabet, the substitution of letters for numbers, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital information content.

In order to easily recover the encrypted information content, the correct decryption key is required. The key is an algorithm that decodes the work of the encryption algorithm. The more complex the encryption algorithm, the more difficult it becomes to decode the communications without access to the key. Generally, there are two types of key schemes for encryption/decryption systems, namely (1) Public Key Systems (PKS) or asymmetric systems which utilize two different keys, one for encryption, or signing, and one for decryption, or verifying; and (2) nonpublic key systems that are known as symmetric, or secret key, systems.

Although the use of public or private key can be an effective way to prevent access to digital content, the transfer of keys often requires extensive coordination with the end user. Also, the use of keys in the related art does not always provide flexible licensing arrangements, or an efficient way to handle many instances of different deliverable digital content products.

Therefore, there is a need to resolve the aforementioned problem relating to conventional approaches for protecting digital information particularly with regard to managing the digital rights for on-line distribution of interactive web content and music.

## SUMMARY OF THE INVENTION

A system for managing rights to a content file within a computer network. The system permits streaming and allows an authorized user to play back the content file

while the user is online. In one embodiment, the system comprises a key for decrypting the content file, a license which contains the key for authorizing decryption and playback of the content file and a header which contains information relating to a name for the license, identification of the content file, and a URL (uniform resource locator) of the server. Advantageously, a content module encrypts the content file, removes a portion of the content file and substitutes the header thereof.

Upon request, a user's computer system receives the content file and the license via a communication network. When the content file and the license have been received, a decoder module decrypts the content file using the key, which is contained within the license. In a further aspect, a license data generator generates a machine identification to which the license is bound so that the content file is playable only on the designated machine. The system further includes a core module for retrieving the identification information from the license data generator, a license database for storing the license when received, and a content player which plays back the content file when it is unencrypted. In this manner, the present invention permits both playback of the content file and management of the corresponding rights to the content file without the disadvantages associated with the related art.

In one embodiment, the present invention provides a system for encrypting a content file within a computer network for on-line playback. The system comprises a first key for decrypting the content file and a header which contains information that allows playback of the content file. Other components include a key module for generating the first key, and a content module for encrypting the content file, and for removing a first content portion of the content file and substituting the header thereof.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A is an illustration of computer system 1 including display 3 having display screen 5.

Fig. 1B illustrates subsystems that might typically be found in a computer such as computer 1.

Fig. 1C is a generalized diagram of a typical network.

Fig. 2 is a block diagram of a zipLock system for encrypting content files according to the present invention.

Fig. 3 is a schematic block diagram of a zipLock delivery system for delivering encrypted content to an end user disk.

Fig. 4 is a schematic block diagram of a zipLock system for enabling playback of content files according to the present invention.

5 Fig. 5 is a block diagram of a zipLock system for acquiring a license which authorizes a user to playback a content file.

#### DETAILED DESCRIPTION OF THE DIAGRAMS

##### 10 Overview

A system for managing the rights to one or more digital content files within a computer network, and for permitting the on-line playback of such content files by an authorized user. In order to manage these rights, the system encrypts the content files to prevent unauthorized access to the files. Encryption is accomplished by using one  
15 or more keys which are associated with one or more segments of the content file. These keys enable an authorized user to decrypt and playback the content files at a subsequent time. Upon receiving the keys, an end user's system retrieves a license from a license server which specifies the rights of the user as it relates to the content files.

Therefore, at the very least, one or more keys and a license are required in  
20 order for a user to play back a content file. In this manner, the present system manages digital rights pertaining to such content files in accordance with one embodiment of the present invention. The present invention will be further understood with reference to the diagrams and descriptions which follow.

##### 25 Description of Hardware

Fig. 1A is an illustration of computer system 1 including display 3 having display screen 5. Cabinet 7 houses standard computer components (not shown) such as a disk drive, CDROM drive, display adapter, network card, random access memory (RAM), central processing unit (CPU), and other components, subsystems and devices.  
30 User input devices such as mouse 11 having buttons 13, and keyboard 9 are shown. Other user input devices such as a trackball, touch-screen, digitizing tablet, etc. can be used. In general, the computer system is illustrative of but one type of computer system, such as a desktop computer, suitable for use with the present invention. Computers can be

configured with many different hardware components and can be made in many dimensions and styles (e.g., laptop, palmtop, pen top, server, workstation, mainframe). Any hardware platform suitable for performing the processing described herein is suitable for use with the present invention.

5           Fig. 1B illustrates subsystems that might typically be found in a computer such as computer 1.

          In Fig. 1B, subsystems within box 20 are directly interfaced to internal bus 22. Such subsystems typically are contained within the computer system such as within cabinet 7 of Fig. 1A. Subsystems include input/output (I/O) controller 24, System  
10 Random Access Memory (RAM) 26, Central Processing Unit (CPU) 28, Display Adapter 30, Serial Port 40, Fixed Disk 42 and Network Interface Adapter 44. The use of bus 22 allows each of the subsystems to transfer data among the subsystems and, most importantly, with the CPU. External devices can communicate with the CPU or other subsystems via bus 22 by interfacing with a subsystem on the bus. Monitor 46 connects  
15 to the bus through Display Adapter 30. A relative pointing device (RPD) 48 such as a mouse connects through Serial Port 40. Some devices such as Keyboard 50 can communicate with the CPU by direct means without using the main data bus as, for example, via an interrupt controller and associated registers (not shown).

          As with the external physical configuration shown in Fig. 1A, many  
20 subsystem configurations are possible. Fig. 1B is illustrative of but one suitable configuration. Subsystems, components or devices other than those shown in Fig. 1B can be added. A suitable computer system can be achieved without using all of the subsystems shown in Fig. 1. For example, a standalone computer need not be coupled to a network so Network Interface 44 would not be required. Other subsystems such as a  
25 CDROM drive, graphics accelerator, etc. can be included in the configuration without affecting the performance of the system of the present invention.

          Fig. 1C is a generalized diagram of a typical network.

          In Fig. 1C, the network system 80 includes several local networks coupled to the Internet. Although specific network protocols, physical layers, topologies, and  
30 other network properties are presented herein, the present invention is suitable for use with any network.

          In Fig. 1C, computer USER1 is connected to Server1. This connection can be by a network such as Ethernet, Asynchronous Transfer Mode, IEEE standard 1553 bus, modem connection, Universal Serial Bus, etc. The communication link need not be a

wire but can be infrared, radio wave transmission, etc. Server1 is coupled to the Internet. The Internet is shown symbolically as a collection of server routers 82. Note that the use of the Internet for distribution or communication of information is not strictly necessary to practice the present invention but is merely used to illustrate a preferred embodiment, below. Further, the use of server computers and the designation of server and client machines is not crucial to an implementation of the present invention. USER1 Computer can be connected directly to the Internet. Server1's connection to the Internet is typically by a relatively high bandwidth transmission medium such as a T1 or T3 line.

Similarly, other computers at 84 are shown utilizing a local network at a different location from USER1 computer. The computers at 84 are coupled to the Internet via Server2. USER3 and Server3 represent yet a third installation.

Note that the concepts of "client" and "server," as used in this application and the industry, are very loosely defined and, in fact, are not fixed with respect to machines or software processes executing on the machines. Typically, a server is a machine or process that is providing information to another machine or process, i.e., the "client," that requests the information. In this respect, a computer or process can be acting as a client at one point in time (because it is requesting information) and can be acting as a server at another point in time (because it is providing information). Some computers are consistently referred to as "servers" because they usually act as a repository for a large amount of information that is often requested. For example, a World Wide Web (WWW, or simply, "Web") site is often hosted by a server computer with a large storage capacity, high-speed processor and Internet link having the ability to handle many high-bandwidth communication lines.

A server machine will most likely not be manually operated by a human user on a continual basis, but, instead, has software for constantly, and automatically, responding to information requests. On the other hand, some machines, such as desktop computers, are typically thought of as client machines because they are primarily used to obtain information from the Internet for a user operating the machine.

Depending on the specific software executing at any point in time on these machines, the machine may actually be performing the role of a client or server, as the need may be. For example, a user's desktop computer can provide information to another desktop computer. Or a server may directly communicate with another server computer. Sometimes this is characterized as "peer-to-peer," communication. Although processes of the present invention, and the hardware executing the processes, may be characterized

by language common to a discussion of the Internet (e.g., "client," "server," "peer") it should be apparent that software of the present invention can execute on any type of suitable hardware including networks other than the Internet.

Although software of the present invention, may be presented as a single entity, such software is readily able to be executed on multiple machines. That is, there may be multiple instances of a given software program, a single program may be executing on two or more processors in a distributed processing environment, parts of a single program may be executing on different physical machines, etc. Further, two different programs, such as a client and server program, can be executing in a single machine, or in different machines. A single program can be operating as a client for one information transaction and as a server for a different information transaction.

#### **Details of Embodiments of the Present Invention**

A first embodiment of the present invention is incorporated into a product called "zipLock"™ available from a primary company Preview Systems, Inc.® of Sunnyvale, California.

Fig. 2 is a block diagram of zipLock system 200 for encrypting content files according to the present invention. As used herein, the term "content" refers to digital information.

In Fig. 2, among other components, system 200 comprises content builder module 216 for encrypting one or more digital files, DRM encoder 210 for coordinating encryption as well as providing a header, DRM key module 212 for associating the information contained within a content file with a license, and zipLock database 202 for storing key sheaves received from content builder 212.

In a typical content encryption procedure, content builder 216 receives a single unencrypted content file 206 (or multiple unencrypted content files 208) for encryption. Content files 206 may be a musical recording, an audio or video image, which may be from third party sources or directly from the content providers. Upon receiving content file 206, content builder 216 utilizes an encryption algorithm to implement the encryption process. In one embodiment, this process is accomplished by segmenting content file 206 into variable segments, each segment being encrypted with a separate key.

A "key" may be a variable value that is applied to content file 206 using an algorithm to produce encryption text. A single key or multiple keys having constant or

variable lengths may be employed depending on which embodiment is implemented. After the encryption process, the keys are saved in zipLock database 202 for later retrieval during the playback process. In an exemplary embodiment, database 202 is an industry standard database system such as Oracle 8™ available from Oracle, Inc.®

5           Content builder 216 also functions to interact with database 202 to create the necessary information to enable the sale, distribution and tracking of the content within system 200. Advantageously, during the encryption process, content builder 216 removes a portion of content file 206 and in its place inserts a header (not shown), supplied by DRM encoder 210. The removed portion is thereafter added to a license file  
10 for authorizing playback of the content file 206. Therefore, the removed portion is considered part of the keys. Depending on the embodiment being implemented, the removed portion may be added to a pre-configured license, the terms of which are predefined. During the playback process, the pre-configured license is then retrieved when its terms are the same as the user's transaction. Alternatively, the removed portion  
15 may be saved and later added to a license which is generated on the fly during the playback process. In any event, once the license is obtained, the removed portion is thereafter recombined with the original content portion during the playback process.

Advantageously, removing a portion of content file 206 also provides a measure of extra security as the removed portion of content file 206 remains unavailable  
20 until decryption time. Therefore, copying encrypted content to another machine is completely useless without the back binding license. A further reason for removing a portion of content file 206 to accommodate the header is to keep the content file the same length as the original file. In this manner, the process of seeking a specific location in content file 206 during the decryption process is simplified.

25           The header within content file 206 contains information fields such as the license name, the content file identification, and the license server URL (uniform resource locator). The license name field enables content file 206 to be associated with the license file (containing the removed content portion). The content identification field identifies the content file 206 while the license server URL points to the address of the license  
30 server where the license is generated (or located). Although a multiple-field header is not shown, one of ordinary skill in the art will realize that the header may contain multiple fields for identifying various types of information other than those referenced above.

Fig. 3 is a schematic block diagram of zipLock delivery system 300 for delivering encrypted content 304 to an end user disk 310.

In Fig. 3, delivery system 300 includes content server 302 for generating encrypted content 304, interactive web player 312 and DRM proxy 308 which provides an alternate means for retrieving encrypted content 304 from server 302. Although operable in a number of modes, in one embodiment, system 300 functions in an on-line mode. In this mode, content 304 remains on content server 302 and is streamed when requested by the user. That is, content 304 is played back as it arrives on disk 310. One method of achieving this functionality is by using a separate module such as DRM proxy 308 for retrieving the content from content server 302, using a receipt 306. It should be noted that DRM proxy 308 is separate and apart from content player 312 because frequent modifications to the module may be carried out as proves necessary, without modifying other components.

Alternatively, a module which functions as part of the content player 312 may carry out the streaming functionality. Examples of content players which are currently available on the market are Quicktime 4™ available from Apple Computer, Inc.®, RealPlayer™ available from RealNetworks, Inc.® and Shockwave 7™ available from MacroMedia, Inc.®. Further, in the on-line mode also referred to as "pay-to-view" mode, the license is delivered concurrently with content 304. Although not shown, it will be apparent to one of ordinary skill in the art that various permutations of modules and modes for retrieving encrypted content 304 are possible.

Fig. 4 is a schematic block diagram of zipLock system 400 for enabling playback of content files 404 according to the present invention. Advantageously, system 400 allows only authorized users to playback content files in accordance with one embodiment.

System 400 comprises content server 402, among other components, for downloading content files 404 to content player 408 for the purpose of allowing playback of the content files. During playback, content player 408 begins by retrieving a chunk of content from content files 404, each file including a content header (described in Fig. 2) for identifying a license name, a content identification, and a license server URL among other information. Thereafter, the chunk of content is handed over to player module 410, which begins to coordinate the decryption of content files 404. Player module 410 contacts DRM core 414 to request a session key for decrypting the content files. Because the requested key is contained within a license, DRM core 414 must identify the appropriate license and its current location. This is accomplished by reading the content header to identify the license name, the content identification, and a license server 406



wherever the license is located. In some instances, DRM core 414 checks to see whether the license is stored within license store 415 and retrieves the license if found. Otherwise, the identified license server URL is contacted to request a license.

In addition, license data generator 416 provides DRM core 414 with a machine identification which is unique to the end user's machine for comparison with the header information. Using all of the obtained information, DRM core 414 through DRM module 420 contacts license server 406 to request the session key and status data for the given machine. Advantageously, the session key is a single session key, meaning that it enables playback of the encrypted files only for a single session.

To obtain the session key, DRM module 420 responds by directing DRM proxy 422 to contact and obtain a license (which contains the session key) from license server 406. Upon successful verification of the license terms, license server 406 delivers the license that contains the session key. DRM proxy 422 passes the license back to DRM module 420, which in turn forwards it to DRM core 414. DRM core 414 retrieves the session key and passes the key securely back to player module 410. In turn, player module 410 forwards the key and encrypted content files 404 to DRM decoder 412 which executes the decryption process and returns the decrypted files to player module 410. Finally, content player 410 passes the decrypted content files content player 408 for playback.

It should be noted that the preceding steps are only performed for the first chunk of encrypted content after which subsequent chunks are automatically played back. Further, it should be observed that there are implications for the player module 410 when it hands encrypted content to the decoder module 412, because content is encrypted on a frame-by-frame basis. This makes seeking a specific location and the content a little more difficult and, as such, the decoder module may be provided with API (application programming interface) to aid the caller in dealing with these frames. In this manner, the present invention enables system 400 to upload encrypted content files 404 and play back those content files using a content player module 410.

Fig. 5 is a block diagram of zipLock system 500 for acquiring a license which authorizes user playback of a content file.

In Fig. 5, as shown in an exemplary embodiment, system 500 includes client and server sides 522 and 520. Among other components, client side 522 includes DRM proxy 504 for preparing data for a license request, module 506 for building a

license request message, DRM core 508 for obtaining machine specific information from license data generator 510, and license database 512 for storing license files.

In a typical operation, the user purchases content such as music recordings (for example) from the store front at a website (not shown). Numerous websites are available for purchasing various types of digital content including Disney.com®, Sony.com®, and Shockwave.com®, for example. Using a web browser or a program that is capable of posting a web form to server 516, the user initiates the transaction with the appropriate website. The transaction typically involves several round trips to the web site with the transaction concluding with a request for a box file 502. Box file 502 is a file that describes the content requested by the user, and in one embodiment has a .cBox extension.

DRM proxy 504 contains a box file handler and is registered with system 500 as the handler for files with the .cBox extension. When box file 502 is received, DRM proxy 504 directs module 506 to build a license request message for forwarding to license server 516. In one embodiment, this request is in XML (extensible markup language) format. Module 506 queries the machine identification to be included in the license request. Thereafter, DRM proxy 504 starts a network job which sends the license request message to license server 516. License server 516, in one embodiment is a CGI (common gateway interface) program available through license server 516.

Upon receipt of the license request, license server 516 verifies that the content file has been purchased prior to continuing with the processing of the license request. zipLock data base 514 contains the terms of the license along with the keys for decrypting the content file. These terms are retrieved and forwarded to license generator 518. It should be observed that a different license generator is implemented for each digital rights management solution being employed on client side 522. License generator 518 generates the license which includes the terms of the license. Also included within the license, are the keys for decrypting the content file.

It should be observed that the content decryption keys are bound to the particular machine located on the client side 522. By way of example, particular information that is unique to the machine such as the machine identification number is bound to the license. In this way, the present invention implements a machine-binding solution which allows digital content playback only on a particular machine. Upon receiving the license from license generator 518, license server 516 forwards the license over the network to DRM proxy 504. In turn, DRM proxy forwards the license to module

506 for DRM-specific processing. DRM core 508 retrieves the license and stores the license within database 512.

Although not shown, the process for retrieving a license may occur subsequent to a purchase transaction such as when the user wishes to play back content offline. Further, license acquisition can also occur when there is no financial transaction involved; for example, when the user requests a trial license. A trial license permits a user to utilize the content files for a specific period after which the trial license expires. Table 1 below illustrates exemplary steps taken by system 500 to acquire a license when there is no financial transaction involved.

10

1.	A content player (not shown) asks DRM core 508 to play a content.
2.	DRM core 508 checks its local store, e.g., license store 512, and finds there is no valid license available (it finds no license or license is expired).
3.	DRM core 508 fields a license request message with the machine identification.
4.	DRM core 508 invokes DRM proxy 504 to send a license request message.
5.	DRM proxy starts a network job to send a license request message to license server 516.
6.	License server 516 presents a page to collect license terms desired by the user and supported by system 500 before continuing with the processing of license request.
7.	The terms of the license are collected and sent to data base 514.
8.	The license request, along with the terms of the license and keys for decryption, are retrieved from data base 514 and are dispatched to license generator 518.
9.	The license is generated from the obtained information.
10.	The license data is returned to server 516.
11.	License data is returned over the network to the DRM proxy 504.
12.	DRM proxy 504 passes the license response message to DRM 506 for DRM-specific processing.
13.	DRM module 506 via DRM core 508 saves the license data in its license store 512 in its own specific way.

**Table 1**

The present invention advantageously separates a portion of the content from the original content file until decryption time to prevent unauthorized content usage. Moreover, licenses are bound to particular machines so that copying the content to a machine other than the authorized machine is futile. The present invention also utilizes a  
5 secure data channel in which the content keys are passed in secured format. Code obfuscation is used to hide code that handles decrypted data.

Other advantages include the implementation of the DRM core and the DRM decoder within separate modules to increase the complexity for hackers, and the employment of session key-based on-line license verification to maximize security. In  
10 this manner, the system of the present invention manages rights to one or more digital content files within a computer network and limits the playback of such content files to an authorized user. Furthermore, the present invention facilitates distribution and content production, which ultimately results in a shorter product development cycle.

While the above is a complete description of exemplary specific  
15 embodiments of the invention, additional embodiments are also possible. Thus, the above description should not be taken as limiting the scope of the invention, which is defined by the appended claims along with their full scope of equivalents.

WHAT IS CLAIMED IS:

- 1                   1.     A system for encrypting a content file within a computer network  
2     for on-line playback, the system comprising:  
3                   a first key for decrypting the content file;  
4                   a header which contains information that allows playback of the content  
5     file;  
6                   a key module for generating the first key; and  
7                   a content module for encrypting the content file, and for removing a first  
8     content portion of the content file and substituting the header thereof.
- 1                   2.     The system of claim 1 further comprising  
2                   a license that contains both the first key and the first content portion.
- 1                   3.     The system of claim 1 wherein the information is any one of a  
2     name for a license, an identifier for the content file, and an URL (uniform resource  
3     locator) of a license server for generating the license.
- 1                   4.     The system of claim 1 wherein the content module segments the  
2     content file into first and second segments.
- 1                   5.     The system of claim 4 further comprising  
2                   a second key, wherein the content module encrypts the first and  
3     second segments of the content file using the first and second keys, respectively.
- 1                   6.     A method by a computer system, for encrypting a content file to  
2     permit on-line play back of the content file, the method comprising:  
3                   generating a first key for decrypting the content file;  
4                   creating a header which contains a first field that contains information for  
5     enabling playback of the content file;  
6                   removing a first portion of the content file and substituting the header  
7     thereof; and  
8                   encrypting the content file such that the content file is decrypt-able using  
9     the first key.
- 1                   7.     The method of claim 6 further comprising

2 including the first portion and the first key in a license for  
3 authorizing playback of the content file.

1 8. The method of claim 6 further comprising  
2 receiving the license containing the first key and the first portion,  
3 decrypting the content file using the first key, and  
4 combining the first portion with the content file.

1 9. A system for managing rights to a content file within a computer  
2 network, and to permit an authorized user to playback the content file online, the system  
3 comprising:

4 a key for decrypting the content file;  
5 a database for storing the key;  
6 a license having the key for authorizing decryption and playback of the  
7 content file;  
8 a license server system having at least one license server, the system  
9 generating the license for forwarding to the authorized user;  
10 a first computer system for generating the content file, the first computer  
11 system further comprising,  
12 a header which contains information relating to a name for the  
13 license, identification of the content file, and an URL (uniform resource locator) of the  
14 license server,  
15 an encoder module for creating the header,  
16 a key module for generating the key,  
17 a content module for encrypting the content file using the key, and  
18 for removing a portion of the content file and substituting the header thereof;  
19 a communication network for streaming the content file and transmitting  
20 the license to the authorized user;  
21 a second computer system for receiving the content file and the license via  
22 the communication network, the second computer system further comprising,  
23 a decoder module for decrypting the content file using the key,  
24 upon receipt of the license;

25                   a license data generator for generating identification information  
26   about a computer wherein the content file is played back,  
27                   a core module for retrieving the identification information from the  
28   license data generator,  
29                   a license database for storing the license when received;  
30                   a content player which plays back the content file when  
31   unencrypted,  
32                   a proxy module for sending a request to obtain the license from the license  
33   server; and  
34                   a request module for forwarding the request to obtain the license to the  
35   proxy module.

1                   10.   The system of claim 9 wherein the license server system  
2   dynamically generates the license when requested by the authorized user while online.  
1                   11.   A system for managing rights to a content file within a computer  
2   network, and to permit an authorized user to playback the content file online, the system  
3   comprising:  
4                   a key for decrypting the content file;  
5                   a first content portion which is part of the content file;  
6                   a license for decrypting the content file, the license containing both the  
7   key and the first content portion;  
8                   a license server system having at least one license server, the system  
9   generating the license for forwarding to the authorized user;  
10                  a first computer system for generating the content file, the first computer  
11   system further comprising,  
12                  a header which contains a first field for having identification  
13   information;  
14                  software containing one of more instructions for creating the  
15   header,  
16                  software containing one or more instructions for generating the  
17   key,  
18                  software containing one or more instructions for encrypting the  
19   content file, and for removing the first content portion from the content file and  
20   substituting the header thereof;

21 a communication network for transmitting the content file and the license;  
22 and  
23 a second computer system for receiving the content file and the license via  
24 the communication network, the second computer system further comprising,  
25 software containing one or more instructions for streaming the  
26 content file while the user is online, and to permit playback of the content file when  
27 unencrypted,  
28 software containing one or more instructions for decrypting the  
29 content file using the key, upon receipt of the license, and  
30 software containing one or more instructions for combining the  
31 first content portion with the content file.

1 12. In a computer network, a method using a license for enabling  
2 playback of a content file, the content file containing a header which identifies the license  
3 and the content file, the license including both a first portion of the content file and a  
4 session key that enables decryption of the content file, the method comprising:  
5 streaming the content file to an authorized user system;  
6 retrieving the license which contains the session key and the first portion  
7 of the content;  
8 for a single playback session, decrypting the content file using the session  
9 key; and  
10 combining the first portion with the content file during playback.

1 13. The method of claim 12 further comprising  
2 dynamically generating the license prior to the step of retrieving  
3 the license.

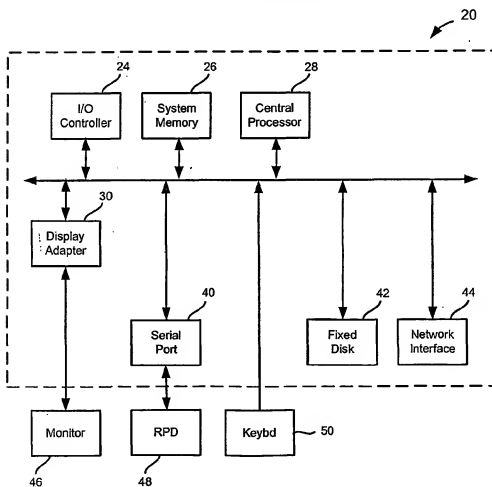
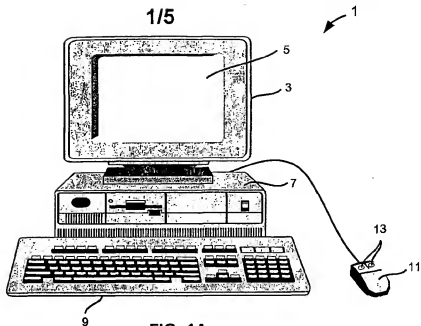
1 14. The method of claim 12 further comprising  
2 storing the license prior to the step of retrieving the license.

1 15. In a computer network, a method for obtaining a license from a  
2 license server to authorize on-line playback of a content file, the license containing a  
3 session key and a portion of the content file, the method comprising:  
4 requesting the license from the license server;



5                   providing the license server with information relating to the terms of the  
6   license and a machine identification wherein the content file is played back;  
7                   binding the license to a machine with the machine identification so that the  
8   content file is playable only on the machine so designated; and  
9                   forwarding the license having the session key and the portion of the  
10   content file to the machine.

1                   16.   The method of claim 15 further comprising  
2                   obtaining a box receipt file prior to the step of requesting the license from  
3   the license server.



2/5

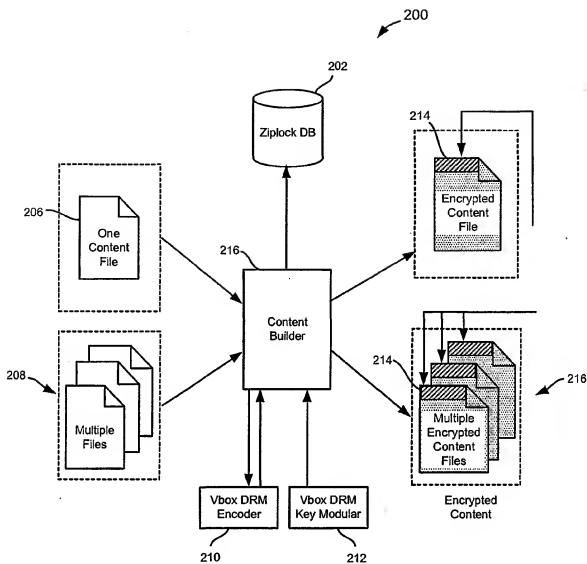


FIG. 2

3/5

300

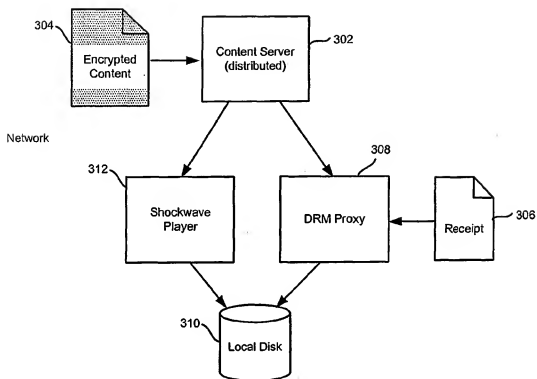


FIG. 3

4/5

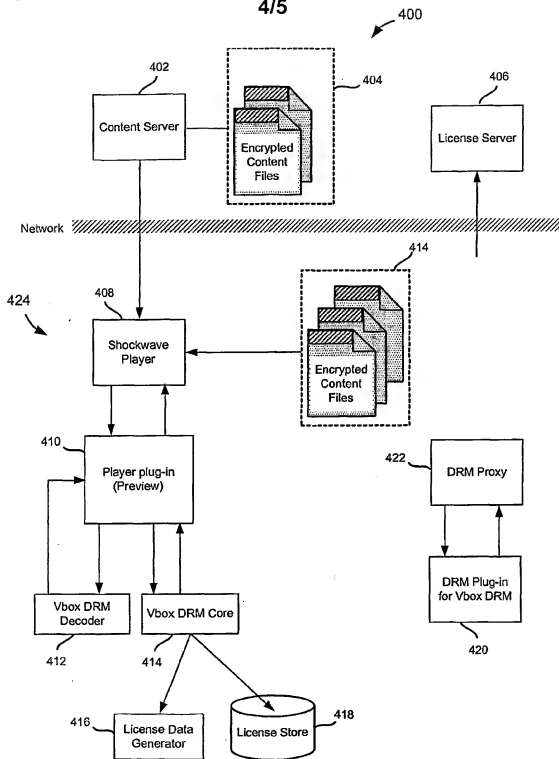


FIG. 4

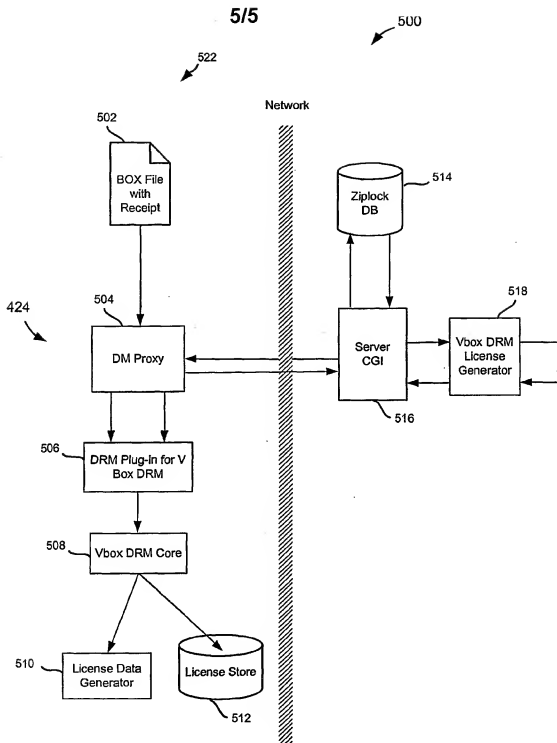


FIG. 5

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau

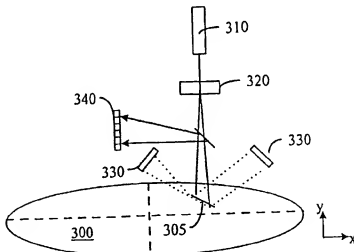
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : <b>G01N 21/88, H01L 21/66</b>	<b>A1</b>	(11) International Publication Number: <b>WO 00/68673</b> (43) International Publication Date: 16 November 2000 (16.11.00)
(21) International Application Number: <b>PCT/US00/13042</b> (22) International Filing Date: <b>11 May 2000 (11.05.00)</b> (30) Priority Data: 09/309,358      11 May 1999 (11.05.99)      US (71) Applicant: <b>APPLIED MATERIALS, INC.</b> [US/US]: 3050 Bowers Avenue, Santa Clara, CA 95054 (US). (72) Inventors: <b>REINHORN, Silviu</b> ; Tavor Street #7, Mevaseret-Zion 90805 (IL). <b>ALMOGY, Gilad</b> ; Poslei Harakevet Street 8, Givatayim 53257 (IL). (74) Agents: <b>BERNADICOU, Michael, A. et al.</b> ; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).	(81) Designated States: JP, KR, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published <i>With international search report.          Before the expiration of the time limit for amending the          claims and to be republished in the event of the receipt of          amendments.</i>	

(54) Title: INSPECTION SYSTEMS PERFORMING TWO-DIMENSIONAL IMAGING WITH LINE LIGHT SPOT

## (57) Abstract

A wafer inspection system is described. The wafer is illuminated by an elongated "linear" or "line spot". The "line spot" is basically an elongated illumination on the wafer surface, such that it covers several pixels aligned to form a line. The linear spot is held stationary with respect to one direction, but the wafer is scanned under it in the other direction. Thus, a two dimensional area is covered and can be imaged. Imaging is preferably performed using a sensor array, such as a line CCD. In the preferred embodiment, two linear spots are used in conjunction with two line CCD's. When inspecting a patterned wafer, the linear spots are projected at complementing 45° angles to the "streets and avenues" axis of the wafer.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SE	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakhstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LJ	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		



INSPECTION SYSTEMS PERFORMING TWO-DIMENSIONAL  
IMAGING WITH LINE LIGHT SPOT

Field of the Invention

5 This invention relates to the systems for inspection of substrates, especially semiconductor wafers and reticles. More specifically, the invention relates to a novel system which illuminates lines of pixels on the substrate, and images reflected and/or scattered light from the lines.

10 Background of the Invention

Several systems are known in the art for the inspection of wafers and reticles. Two example of such systems are depicted in Figures 1 and 2. In the system exemplified in Figure 1, the wafer 100 is illuminated with a light beam emanating from a light source 110 and reaching the wafer at 15 90° angle (generally referred to as normal illumination). Preferably, light source 100 provides coherent light, i.e., source 100 may be a laser source. The light beam is scanned over the wafer by a scanner 120, typically an acousto-optical scanner (AOD) or a rotating mirror, in the direction marked by the double-headed arrow. The wafer 100 is moved in the 20 perpendicular direction by moving the stage upon which the wafer rests. Thus, a two dimensional area of the wafer can be scanned by the light beam.

Since the wafer has basically a mirror-like top surface, the light beam 25 specularly reflects back per Snell's law at 180°. This specularly reflected light is collected by a light sensor 140 and its signal is used to obtain a "bright field" image, i.e., an image created from specularly reflected light. However, whenever the light beam hits an irregularity on the wafer, such

as a particle or etched pattern, the light scatters in various directions. Some of the diffracted/scattered light is then collected by the light sensors 130, and their signal is used to obtain a "dark field" image, i.e., an image created from diffracted/scattered light. Thus, when the wafer has no  
5 pattern on it (e.g., blank wafer), the irregularities appear in the dark field image as stars in a dark sky. When the wafer has a pattern on it, the irregularities cause a scattered light which deviates from the normal diffraction caused by the pattern.

10 In the system exemplified in Figure 2, the wafer 200 is illuminated by a light beam emanating from light source 210, but reaching the wafer at a shallow angle, generally referred to as grazing illumination. The light beam is scanned over the wafer by a scanner 220, typically an acousto-optical scanner or a rotating mirror, in the direction marked by the  
15 double-headed arrow. The wafer 200 is moved in the perpendicular direction by moving the stage upon which the wafer rests. Thus, a two dimensional area of the wafer can be scanned by the light beam.

Since the light reaches the wafer at a grazing angle  $\theta$ , its specular reflection is at a corresponding angle,  $\theta'$ , according to Snell's law. This  
20 light can be collected by sensor 240, and its signal is used to create the bright field image. Any diffracted/scattered light is collected by sensors 230, the signal of which is used to create dark field images.

25 It should be appreciated that in the above exemplified systems, with respect to each sensor the image data is acquired serially. That is, each two dimensional image, whether bright or dark field, is constructed by acquiring signals of pixel after pixel, per the scanned light beam. This is

time consuming serial operation, which directly affects the throughput of such systems. Moreover, the scan speed of such systems is limited by the scanner's speed (i.e., the band-width for an acousto-optic scanner) and by the electronics that support the detectors, e.g., the PMT (Photo-Multiplier Tube). Thus, a need exists to develop a system that does not utilize a scanned light beam.

Looking forward, as design rules shrink, the importance of detecting increasingly small irregularities becomes paramount. With design rules such as 0.18 and 0.15  $\mu\text{m}$ , very small irregularities, such as particles of sub-micron size, can be killer defects and cause the device to malfunction. However, in order to detect such small irregularities, one needs to use a very small wavelength light source, such as ultra violet (UV) or deep ultra violet (DUV) light source. This presents at least two crucial problems: first, optical elements operating in the DUV regime are expensive and, second, small short wave implies small spot size of the light beam; thus, the scanning speed and collection data rate need to be increased.

Currently, commercially available AOD that can support a scanning for a DUV beam have a very limited performance. Additionally, even if such AOD can be developed, at present it is unclear whether it could withstand the energy levels required for obtaining a high resolution image using a DUV light beam. Thus, reducing the power level may also dictate use of a slower scanning AOD. Therefore, future systems may also require implementations that do not rely on beam scanning.

#### Summary of the Invention

According to the present invention, the wafer is illuminated by an elongated "linear" or "line spot." The "line spot" is basically an elongated illumination on the wafer surface, such that it covers several pixels aligned to form a line. In the preferred embodiment, the number of pixels  
5 in the linear spot is on the order of thousands. The linear spot is held stationary with respect to one direction, but the wafer is scanned under it in the other direction. Thus, a two dimensional area is covered and can be imaged. Imaging is preferably performed using a sensor array, such as a line CCD. In the preferred embodiment, two linear spots are used in  
10 conjunction with two line CCD's. The detected lateral pixel size (along the narrow dimension of the line) is determined by the illumination line width. The detected pixel size along the longitudinal direction is determined by the resolution of the collection optics and the line CCD camera pixel size. When inspecting a patterned wafer, the linear spots  
15 are projected at complementing 45° angles to the "streets and avenues" axis of the wafer.

The present invention is advantageous in that it enables much faster data acquisition rate. Furthermore, it is operable with short wavelengths, such  
20 as UV or deep UV illumination. Notably, the inventive system does not require a scanning mechanism. Other advantages of the invention will appear as the description proceeds.

#### **Brief Description of the Drawings**

25 In the drawings:

- Figure 1 is a schematic representation of prior art wafer inspection system using normal illumination;

- Figure 2 is a schematic representation of another prior art wafer inspection system, using grazing angle illumination;

- Figure 3 is a schematic representation of a first embodiment of the present invention.

5       - Figure 4 is a top view of the elements of the system depicted in Figure 3, which are relevant for the understanding of the dark field imaging.

10       - Figure 5 is a side view of the elements of the system depicted in Figure 3, which are relevant for the understanding of the bright field imaging.

- Figure 6 is a schematic representation of another embodiment of the present invention, employing four dark field detectors.

15       - Figure 7 is a schematic representation of the preferred embodiment of the present invention, employing dark and bright field detectors.

- Figure 8 exemplifies an optical system for converting the light beam into a linear beam.

- Figure 9 depicts a manner of two-dimensional imaging of a wafer.

20       - Figures 10 and 11 depict two arrangement of Scheimpflug imaging.

#### Detailed Description of Preferred Embodiments

Before, proceeding with the description of the preferred embodiments, it should be noted that any of the embodiments are suitable for inspection of un-patterned wafers. However, several notable advantages of the invention are particularly useful for the more complicated task of patterned wafers inspection. Therefore, much of the discussion presented herein relates to patterned wafers.

25

Figure 3 depicts a simplified version of the present invention. The wafer 300 is illuminated by a linear spot 305 impinging in normal direction with respect to the wafer, created by a light source 300 and suitable optics 320.

5 In the preferred embodiment, the linear spot is held stationary, while the wafer is scanned in the y direction by moving the stage. Thus, a two dimensional strip is scanned over the wafer without the need for scanning the spot in the x direction. The dimensions of the scanned strip are defined by the effective size of the linear spot..

10 Specularly reflected light from the linear spot is then imaged on a sensor array 340, and diffracted light is imaged on sensor arrays 330. Thus, bright and dark field images can be obtained at a fast rate, since the images are sampled one line at a time, rather than one pixel at a time.

15 That is, each sampling of a sensor array provides pixel data for an entire line, the width of the scanned strip. Since sensor arrays of 1024, 2048 and 4096 pixels are widely available off the shelf, the speed of image acquisition can be dramatically increased using the invention. For example, using a sensor array having 2048 pixels with 16 channels, one

20 can achieve acquisition speed of 400Mb/s.

Another feature of the present invention is exemplified in Figure 3. As is well known, one difficulty in inspecting patterned wafers is that features constructed on the wafer, such as metal lines, also diffract light. This

25 causes at least two problems. As far as bright field image is concerned, strong reflections from metals line saturate the light sensor, so that irregularities laying close to the line may go undetected. As far as dark field is concerned, diffraction from metal lines can be mistaken by the

system for irregularities. Thus, in order to avoid these problems, in the preferred embodiment depicted in Figure 3, the linear spot is projected at 45° angle to the streets and avenues (shown in broken lines) of the patterned wafer. Consequently, with respect to the bright field image, instantaneous reflections from metal lines are minimized and, with respect to dark field images, diffraction from metal lines is avoided in the direction of the sensors.

The above feature is exemplified in more details in Figure 4, which is a top view of the inventive system of Figure 3. Specifically, linear spot 305 is depicted as being at 45° angle to the x-y axis (i.e., the streets and avenues directions of the wafer). On either side of the linear spot, objectives 315 are used to image the spot onto the line sensors 330. Of course, so long as no regularity is present, i.e., no light is diffracted, the image projected by the objectives 315 would mostly be dark. However, when irregularity is present, the light hitting it will be scattered and imaged onto the sensor arrays 330. Depending on the size of the irregularity, the bright image can appear on only a single or on several elements of the sensor array. The detected pixel size is determined by two main factors: the illumination line width and the collection optics resolution. The illumination line width is determined by the numerical aperture of the cylindrical lens. However, the detected pixel size in the longitudinal direction is determined by the numerical aperture of the collection optics and the line CCD camera pixel size.

25

Sampling of the bright field image is exemplified in Figure 5, in which elements relating to dark field imaging have been omitted for clarity. Specifically, the illumination light passes through a beam splitter 565 and

objective 545. When the light is reflected, it again passes through the objective 545, but this time it is reflected by the mirror 565 onto lens 575. Lens 575 images the linear spot onto the sensor array 540.

5 While the system thus far described has a vastly increased throughput, in its preferred embodiment it includes two linear spots imaged onto four dark field sensor arrays. This is exemplified in Figure 6, which depicts how the prior art system of Figure 2 can be modified to include the inventive system. However, it should be appreciated that all the  
10 embodiments described herein can be equally applied to any prior art system, including those depicted in Figures 1 and 2.

In Figure 6, the beam provided from light source 610 is split by beam splitter 615. Part of the light is allowed to continue and illuminate a first  
15 linear spot, while the remaining light is reflected by mirror 625 to illuminate a second linear spot. The linear spots are oriented at 45° with respect to the x-y axis of the wafer, but at 90° to each other. Two pairs of sensor arrays image one linear array, while another pair images the other. This configuration provides imaging of each pixel from four  
20 different dark field perspectives.

However, in order to correlate the various perspectives, one need to account for the different imaging locations of the four sensors 630. That is, in inspection systems it is known to perform a die-to-die or a cell-to-cell  
25 comparison of each pixel to detect defects. Thus, for each particular pixel location defined on the wafer, the various perspective images are compared to similar images of a corresponding location in the neighboring preceding and proceeding dies or cells. Thus, for each comparison



operation, the images of the specific pixel location need to be correlated. This operation is schematically illustrated in Figure 6 by showing each sensor 630 connected to a delay line 635. Of course, one may instead perform the delay using an algorithm rather than actual electronic delay. That is, since the collected data is stored in memory, for each pixel location the algorithm can fetch the appropriate data from the appropriate locations in the memory.

It should be appreciated that the two linear spots need not be separated in space and can be crossed instead. However, such an arrangement is not very desirable since it will have higher noise caused by stray light. That is, while one line spot will be properly imaged onto the sensor array, some additional light from the other line spot will also enter the imaging system and may reduce the signal to noise ratio. Therefore, the configuration as shown is preferable. Additionally, a bright field sensor array may be added, although it has been omitted from Figure 6 for clarity. Of course, the inventive system is easily adaptable to inspection systems using UV or DUV coherent light, since there's no limitation on scanning capability and rate.

For the preferred embodiment, it is possible to use off the shelf line CCD's. Such CCD's are currently capable of acquisition rates of 400Mb/sec, provided in 16 parallel channels, i.e., 25Mb/sec/channel. While such data rates are several times the current data acquisition rates, the line CCD's can be custom designed to achieve data rates on the order of 1Gb/sec and even further increase the acquisition rate. Moreover, since the data from the line CCD's is provided in 16 parallel channels, it reduces the load on the collection electronics, since each line can be provided with its own

electronics, thus each electronics package would have to handle only one sixteenth of the overall data rate. Of course, the custom designed CCD's can be designed with a larger number of channels, suitable for the particular system designed.

5

The preferred embodiment of the present invention is depicted in Figure 7. Specifically, Figure 7 depicts a manner of modifying the system of Figure 1 to include the features of the present invention. The system of Figure 7 includes normal illumination from a light source 710. The light from the light source 710 is made into a linear beam by optics 720. Optics 720 can generally comprise elements such as a beam expander, a cylindrical lens, and a cylindrical lens in combination with a slit aperture. An exemplary optics 720 is depicted in Figure 8. Specifically, light from a coherent illumination source is made into an expanded beam 800 by beam expander 815. The expanded beam 800 is passed through a slit aperture 810, and then through a cylindrical lens 820. Thus, a spatially linear beam is obtained. The beam is then split into two beams, each for illuminating one linear spot. Of course, the beam can be first split, and then passed through two optics system to form each beam into a linear beam.

20

As depicted in Figure 7, four dark field light sensor arrays are employed to obtain four dark field perspective. As in Figure 6, the sensor arrays are coupled to delay lines 735, which are implemented in software, hardware, or combination thereof. Additionally, in Figure 7 two bright field sensor arrays are depicted, to obtain two bright field images; however, it is envisioned that a single bright field sensor array would be sufficient.

25

In Figure 7, a two dimensional image is acquired by moving the wafer in the x direction. Specifically, when inspecting a patterned wafer using a die-to-die method, it is preferred to obtain two-dimensional "strip" images. This is exemplified in Figure 9. A patterned wafer 900 includes a plurality of dies 910. Each die is imaged by imaging two-dimensional strips 920. The strips are imaged by two line spot illumination, and motions of the wafer in one direction. Thus, the width of the strip corresponds to the sensor array's size, i.e., the number of pixels imaged width-wise corresponds to the number of sensors in the sensor array. The length of the strip can be set according to the application. In a die-to-die comparison, the length of the strip can be set to cover, for example, three dies.

Another possible configuration for imaging the scattered light from an illuminated line onto a line CCD is schematically depicted in Figures 10 and 11. In this configuration the illumination line 10 is oriented in parallel to one of the die sides. The scattered light is still collected in an angle of 45 degrees with respect to the streets and alleys of the die because of signal to noise issue discussed before. This could be achieved by using Scheimpflug imaging configuration (reference: Rudolf Kingslake, "Optical System Design", Page 58, 270), i.e. the collection imaging lens 11 should be placed in a position in space so that its median plane 12 is perpendicular to the light scattered into the desired direction (45 degrees). The line CCD 13 is oriented so that the continuation of the line CCD and the illumination line cross each other on the median plane. In such a configuration four line CCD can simultaneously collect the scattered light, and there is no need for two illumination lines.

5       While embodiments of the invention have been described by way of illustration, it will be apparent that the invention can be carried into practice with many modifications, variations and adaptations without departing from the scope and spirit of the invention, as defined by the appended claims.

## CLAIMS

1. Method for the illumination of two dimensional area on a substrate having normal direction defined thereupon, comprising the steps of:
- 5           - illuminating a line spot on the substrate;
- scanning the substrate in a single direction; and
- collecting scattered light at an angle to said normal direction.
2. The method according to claim 1, wherein the step of scanning
- 10           comprises moving the substrate in the normal direction as it is being illuminated.
3. The method according to claim 1, wherein the step of scanning
- comprises moving the line spot across the substrate in the normal
- 15           direction.
4. The method according to claim 1, wherein the line spot is oriented at
- 45° with respect to the normal direction.
- 20           5. The method according to claim 1, further comprising imaging light reflected from the line spot onto at least one sensor array.
6. The method according to claim 1, further comprising imaging light
- scattered from the line spot onto at least one sensor array.
- 25           7. The method of claim 1, further comprising illuminating the substrate with a second line spot oriented at 90 degrees with respect to the line spot.

8. The method according to claim 7, further comprising imaging light reflected from at least one of the line spot and second line spot onto at least one sensor array.
- 5
9. The method according to claim 7, further comprising imaging light scattered from the line spot onto at least one sensor array and imaging light diffracted from the second line spot onto at least one another sensor array.
- 10
10. A system for two dimensional imaging of a substrate, said substrate having a major axis defined thereupon, the system comprising:
- a light source providing a light beam;
  - optical system converting the light beam into a line beam and projecting the line beam onto the substrate to illuminate the substrate with a line spot;
  - a scanning system providing a relative displacement between the line beam and the substrate; and,
  - at least one sensor array situated to receive light scattered at an angle to the major axis.
- 15
11. The system of claim 10, wherein said optical system comprises a cylindrical lens.
- 20
12. The system of claim 10, wherein said optical system comprises a slit aperture.
- 25

13. The system of claim 10, wherein said sensor array is positioned to collect light reflected from the substrate.
14. The system of claim 10, wherein said sensor array is positioned to collect light diffracted from the substrate.
- 15
15. The system of claim 10, wherein said scanning system comprises an x-y stage supporting said substrate.
16. A system for two dimensional scanning of a substrate, comprising:
- a light source providing a light beam;
  - a conversion system converting the light beam into a main line beam;
  - a beam splitter splitting the main line beam into a first and a second line beams;
  - a first optical system projecting the first line beam onto the substrate to illuminate the substrate with a first line spot;
  - a second optical system projecting the second line beam onto the substrate to illuminate the substrate with a second line spot;
  - a scanning system providing a relative displacement between the first and second line beams and the substrate; and,
  - a first sensor array associated with the first line spot; and
  - a second sensor array associated with the second line spot.
17. The system of claim 16, wherein said conversion system comprises a cylindrical lens.
- 25

18. The system of claim 16, wherein said conversion system comprises a slit aperture.

19. The system of claim 16, wherein said second line spot is oriented at  
5 ninety degrees to the first line spot.

20. The system of claim 16, wherein said first and second sensor arrays  
comprise line CCD's.

10

21. A system for two dimensional scanning of a substrate having two  
perpendicular axis defined thereon, comprising:

a light source providing a light beam;

15 optical system converting the light beam into a line beam and  
projecting the line beam onto the substrate to illuminate the  
substrate with a line spot positioned at 45° to the axis;

a scanning system providing a relative displacement between  
the line beam and the substrate; and,

at least one sensor array.

20

22. A system for two dimensional imaging of a substrate having two  
perpendicular axis defined thereon, comprising:

a light source providing a light beam;

25 a conversion system converting the light beam into a main line  
beam;

a beam splitter splitting the main line beam into a first and a  
second line beams;



a first optical system projecting the first line beam onto the substrate to illuminate the substrate with a first line spot positioned at  $45^{\circ}$  to the axis;

5 a second optical system projecting the second line beam onto the substrate to illuminate the substrate with a second line spot, positioned at  $90^{\circ}$  to the first line spot;

a scanning system providing a relative displacement between the first and second line beams and the substrate; and,

10 a first sensor array associated with the first line spot; and  
a second sensor array associated with the second line spot.

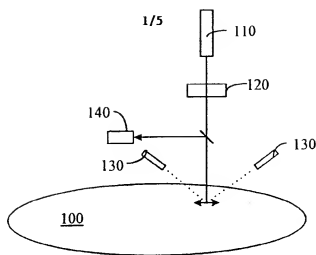


Figure 1

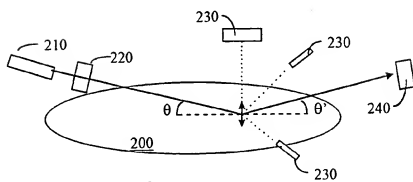


Figure 2

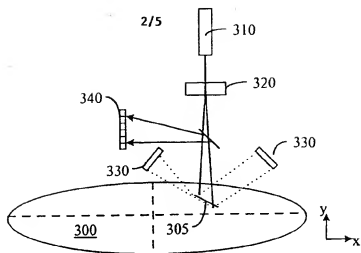


Figure 3

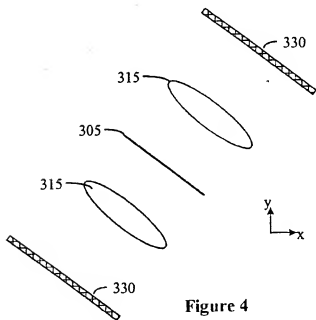


Figure 4

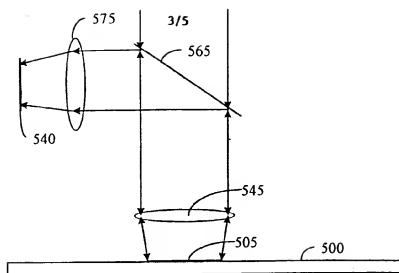


Figure 5

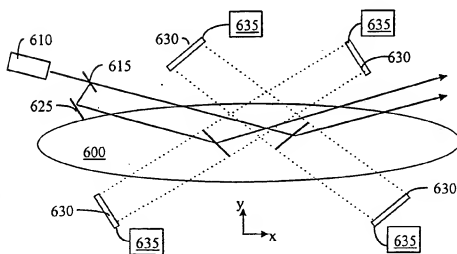


Figure 6

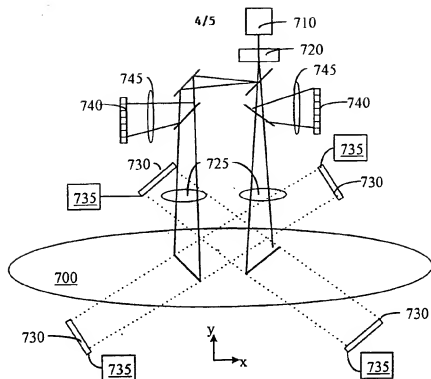


Figure 7

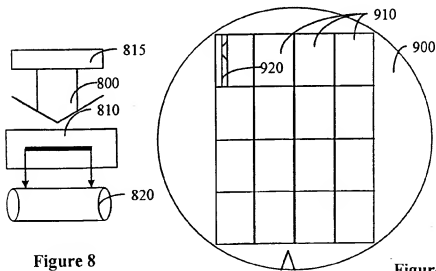
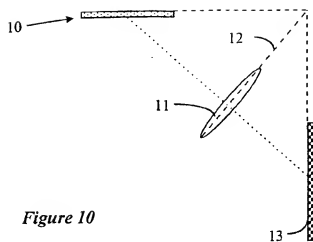
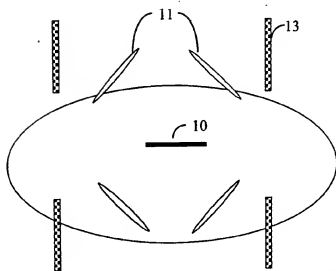


Figure 8

Figure 9

5/5

*Figure 10**Figure 11*

## INTERNATIONAL SEARCH REPORT

In tional Application No  
PCT/US 00/13042

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 7 G01N21/88 H01L21/66

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G01N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99 06823 A (KLA-TENCOR) 11 February 1999 (1999-02-11) page 8, line 1 - line 20; figure 1	1,10,21
X	US 5 274 434 A (HITACHI) 28 December 1993 (1993-12-28) column 8, line 64 -column 9, line 6; figure 7	1,10,21
A	WO 99 14575 A (KLA-TENCOR) 23 March 1999 (1999-03-23) page 13, line 30 -page 14, line 7; figure 3	16,22
P,X	WO 99 38002 A (APPLIED MATERIALS) 29 July 1999 (1999-07-29) page 16, line 4; claim 1; figure 7	1,10,16, 21,22
	—/—	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

\* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubt on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document relating to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"S" document member of the same patent family

Date of the actual completion of the international search

1 September 2000

Date of mailing of the international search report

14/09/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5018 Patentaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Mielke, W

## INTERNATIONAL SEARCH REPORT

International Application No.  
PCT/US 00/13042

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 856 868 A (NIKON) 5 January 1999 (1999-01-05) figure 1	
A	US 5 631 733 A (PHOTON DYNAMICS) 20 May 1997 (1997-05-20) figure 7	
A	WO 98 20327 A (KLA-TENCOR) 14 May 1998 (1998-05-14) figure 2A	



## INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. Patent Application No.  
PCT/US 00/13042

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9906823	A	11-02-1999	AU 8765798 A EP 1000346 A	22-02-1999 17-05-2000
US 5274434	A	28-12-1993	JP 3285339 A JP 2843424 B JP 4056245 A JP 4152545 A US 5463459 A US 5233191 A KR 9513433 B	16-12-1991 06-01-1999 24-02-1992 26-05-1992 31-10-1995 03-08-1993 08-11-1995
WO 9914575	A	25-03-1999	AU 9400098 A EP 1023582 A	05-04-1999 02-08-2000
WO 9938002	A	29-07-1999	NONE	
US 5856868	A	05-01-1999	JP 10026589 A JP 10026590 A	27-01-1998 27-01-1998
US 5631733	A	20-05-1997	WO 9622520 A	25-07-1996
WO 9820327	A	14-05-1998	US 5917588 A AU 5103798 A EP 0935747 A	29-06-1999 29-05-1998 18-08-1999